Resistance against Adaptive Plaintext-Ciphertext Iterated Distinguishers ⋆ ⋆⋆

Aslı Bay[1], Atefeh Mashatan[2], and Serge Vaudenay[1]
Speaker:

[1] EPFL, Switzerland,
{asli.bay, serge.vaudenay}@epfl.ch
[2] Security Engineering, Canadian Imperial Bank of Commerce (CIBC), Canada,
Atefeh.Mashatan@cibc.com

Abstract. Decorrelation Theory deals with general adversaries who are mounting iterated attacks, i.e., attacks in which an adversary is allowed to make d queries in each iteration with the aim of distinguishing a random cipher C from the ideal random cipher C^*. A bound for a *non-adaptive* iterated distinguisher of order d, who is making *plaintext (resp. ciphertext)* queries, against a $2d$-decorrelated cipher has already been derived by Vaudenay at EUROCRYPT '99. He showed that a $2d$-decorrelated cipher resists against iterated non-adaptive distinguishers of order d when iterations have almost no common queries. More recently, Bay et al. settled two open problems arising from Vaudenay's work at CRYPTO '12, yet they only consider non-adaptive iterated attacks.
Hence, a bound for an *adaptive* iterated adversary of order d, who can make both *plaintext* and *ciphertext* queries, against a $2d$-decorrelated cipher has not been studied yet. In this work, we study the resistance against this distinguisher and we prove the bound for an adversary who is making adaptive plaintext and ciphertext queries depending on the previous queries to an oracle.

1 Introduction

Attempting to provide provable security to block cipher cryptanalysis, Nyberg [Nyb91] pioneered a new direction where the notion of strength against differential cryptanalysis is formally examined. Similarly, Chabaud and Vaudenay [CV94] examined the notion of strength against linear cryptanalysis. Luby and Rackoff [LR85,LR86] have also considered a Feistel scheme with a random round function and defined the notion of k-wise

⋆ This work was supported in part by the European Commission through the ICT program under contract ICT-2007-216646 ECRYPT II.
⋆⋆ This work was supported by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center of the SNF under grant number 5005-67322 when the second author was at EPFL.

independent hash function families. The caveat with their approach is that very long secret keys are required. Carter and Wegman [CW79,CW81], however, require smaller key when measuring the effects of pseudorandomness against the adversaries.

Inspired by the notion of k-wise independence of Luby and Rackoff and the derandomization techniques of Carter and Wegman in sampling pairwise independent numbers, Vaudenay defined and formalized Decorrelation Theory [Vau99c,Vau03] to provide provable security for block ciphers against a wide range of statistical attacks. Indeed perfect decorrelation of order d is equivalent to the d-wise independence of Luby and Rackoff while appropriate norms and measures are defined for imperfect decorrelation in [Vau98a,Vau99a]. Moreover, Decorrelation Theory covers a variety of statistical attacks such as Differential and Linear Attacks, Boomerang Attacks, Truncated Differential Attacks, and Impossible Differential Attacks. However, the attacks covered in Decorrelation Theory are generic attacks complying a certain broad criteria in the Luby and Rackoff model.

Decorrelation Theory considers computationally unbounded attackers who can make d queries in each iteration. When these d queries are random and independent from one another, the attacker is a d-limited *non-adaptive* adversary. In contrast, one can consider *adaptive* adversaries who choose their queries depending on the previous ones. Then, a distinguisher of order d is trying to distinguish between a random cipher C and the ideal random cipher C^* using the aforementioned adversary.

Non-adaptive iterated distinguishers, making plaintext (resp. ciphertext) queries, have been studied in [Vau98b,Vau99b,Vau99c,Vau98a,BV05] extensively, and the security of many block ciphers has been proven by decorrelation techniques, see for example [PV98,Vau03,BF06a,BF06b]. In particular, Vaudenay [Vau99c,Vau03] finds an upper bound for the advantage of a non-adaptive iterated distinguisher of order d, who is making plaintext (resp. ciphertext) queries against a $2d$-decorrelated cipher. He shows that a $2d$-decorrelated cipher resists against iterated non-adaptive attacks of order d when iterations have almost no common queries. His work has been followed by Bay et al. [BMV12] who address two open problems arising from Vaudenay [Vau99c,Vau03] on non-adaptive iterated attacks. When considering resistance against non-adaptive iterated adversaries of order d who are making only plaintext (resp. ciphertext) queries, Bay et al. showed that not only it is sufficient for a cipher to have decorrelation of order $2d$, but this decorrelation order is also necessary.

Moreover, they proved that repeating a plaintext query in different iterations may provide a significant advantage to a non-adaptive adversary.

However, a bound for the advantage of an *adaptive* iterated distinguisher of order d, who can make both *plaintext* and *ciphertext* queries has not been computed yet. The significance of studying general distinguishers who can make adaptive queries is not hidden to anyone. Hence, it is important to study adaptive distinguishers. Allowing the adversary to make both plaintext and ciphertext queries strengthens the security results and has already appeared in the literature. Indeed, the Boomerang attack [Wag99] is an example of such an adversary. Studying these general distinguishers making adaptive plaintext-ciphertext queries allows us to, for example, interpret Wagner's Boomerang attack [Wag99] on COCONUT98 [Vau98b,Vau03], a perfect 2-decorrelated block cipher and *provably secure* against differential and linear cryptanalyses and iterated attacks of order 1. Indeed, it could have resisted to Wagner's attack with a decorrelation of order 8.

In this paper, we are going to focus on adaptive iterated distinguishers who can make plaintext and ciphertext queries. We first define a generic adaptive plaintext-ciphertext d-limited distinguisher with an adversary who is making adaptive plaintext queries and ciphertext queries to the oracle depending on the previous queries. We, then, extend this definition to a generic adaptive plaintext-ciphertext *iterated* distinguisher of order d. We prove the bound for the advantage of *adaptive iterated* distinguisher of order d against a $2d$-decorrelated cipher. The appropriate metric for computing the advantage of this kind of adversary was defined by Vaudenay in [Vau99a]. It comes with no surprise that using this metric, we get a looser, i.e., higher, upper bound for adaptive distinguishers than that for non-adaptive distinguishers.

The rest of this paper is organized as follows. Some background results, notations, and definitions are summarized in Section 2. Section 3 defines generic adaptive plaintext-ciphertext iterated distinguishers of order d and Section 4 computes the bound for such adversaries, encapsulating the main contribution of the paper. Appendix A and Appendix B give the details the proof of Theorem 7. Appendix C reminds linear and differential distinguishers.

2 Preliminaries

Vaudenay defines Decorrelation Theory based on the *Luby-Rackoff Model* [LR85] in which the adversary is unbounded in terms of *computational*

power, but bounded in the number of d plaintext-ciphertext queries that he can make. In this model, there is an oracle Ω implementing either an instance of a random function (resp. permutation) drawn from all considered functions (resp. permutations) or an instance of a random function (resp. permutation) drawn uniformly at random from all random functions (resp. permutations). The aim of the adversary $\mathcal{A}$ is to guess which of two distributions the oracle Ω selects. There are two main types of adversaries: when the adversary makes his d queries at the same time and this is called a d-limited *non-adaptive* distinguisher; when the adversary makes queries depending on answers to previous queries and this is called a d-limited *adaptive* distinguisher.

Throughout the paper, F denotes a random function (or equivalently a function set up with a random key) from a set $\mathcal{M}_1$ to a set $\mathcal{M}_2$ while F^* denotes an ideal random function from $\mathcal{M}_1$ to $\mathcal{M}_2$ drawn uniformly at random from all $|\mathcal{M}_2|^{|\mathcal{M}_1|}$ random functions. In addition, C denotes a random cipher (or equivalently the encryption function set up with a random key) over a message space $\mathcal{M}$ and C^* denotes an ideal random cipher over $\mathcal{M}$ drawn uniformly at random from all $|\mathcal{M}|!$ permutations of $\mathcal{M}$. Note that F^* and C^* are also denoted as a *perfect function* and a *perfect cipher*, respectively. In Table 1, we provide some notations to be used throughout the paper.

Table 1. Notations

$\lvert S\rvert$: number of elements in S
$\mathcal{M}^d$: set of all sequences of d tuples over the set $\mathcal{M}$
$[F]^d$: d-wise distribution matrix of a random function F
$\mathrm{Adv}_{\mathcal{A}_{\mathsf{NA}(d)}}$: advantage of the d-limited non-adaptive distinguisher $\mathcal{A}_{\mathsf{NA}(d)}$
$\mathrm{Adv}_{\mathcal{A}_{\mathsf{A}(d)}}$: advantage of the d-limited adaptive distinguisher $\mathcal{A}_{\mathsf{A}(d)}$
$\mathrm{Adv}_{\mathcal{A}_{\mathsf{NAI}(d)}}$: advantage of the non-adaptive iterated distinguisher $\mathcal{A}_{\mathsf{NAI}(d)}$ of order d
$\mathrm{Adv}_{\mathcal{A}_{\mathsf{AI}(d)}}$: advantage of the adaptive iterated distinguisher $\mathcal{A}_{\mathsf{AI}(d)}$ of order d
$\mathbb{E}(X)$: expected value of a random variable X
$V(X)$: variance of a random variable X
$\oplus$: addition modulo 2

Decorrelation Theory has a link with Linear and Differential Cryptanalyses (see Appendix C) which are the essential cryptanalysis methods of both block ciphers and pseudorandom functions. Both methods have iterative analysis of an instance of a block cipher and refer to the set of attacks called *iterated attacks*. More explicitly, iterated attacks are defined

as iterations of d-limited distinguishers. When d-limited *non-adaptive* distinguishers are iterated, we obtain *non-adaptive* iterated distinguishers of order d. When d-limited *adaptive* distinguishers are iterated, we get *adaptive* iterated distinguishers of order d. A generic non-adaptive iterated distinguisher of order d is illustrated in Figure 1. Briefly, a test $\mathcal{T}$ generates the binary output T_i of each iteration i, and then the acceptance set $\mathcal{A}cc$ produces the decision of the distinguisher based on the tuple $(T_1, \ldots, T_n)$.

Input: an integer n, a set X, a distribution $\mathcal{X}$ on X, a test $\mathcal{T}$, a set $\mathcal{A}cc$
Oracle: the oracle Ω implementing a permutation c
for $i = 1$ to n **do**
  pick $x = (x_1, \ldots, x_d)$ at random from $\mathcal{X}$
  get $y = (\Omega(x_1), \ldots, \Omega(x_d))$
  set $T_i = 0$ or 1 such that $T_i = \mathcal{T}(x, y)$
end for
if $(T_1, \ldots, T_n) \in \mathcal{A}cc$ **then**
  output 1
else
  output 0
end if

Fig. 1. A generic non-adaptive iterated distinguisher of order d

The success of an adversary is often estimated by a measure called *advantage* defined as follows.

Definition 1. *Let F_0 and F_1 be two random functions. The* advantage *of an adversary $\mathcal{A}$ distinguishing F_0 from F_1 is defined by*

$$\mathrm{Adv}_{\mathcal{A}}(F_0, F_1) = \big|\Pr[\mathcal{A}(F_0) = 1] - \Pr[\mathcal{A}(F_1) = 1]\big|.$$

When we consider all adversaries distinguishing between F_0 and F_1 and take the maximum of the advantage over all these adversaries in a class ζ, we get the *best advantage* of the distinguisher which is formulated as follows.

$$\mathrm{BestAdv}_{\zeta}(F_0, F_1) = \max_{\mathcal{A} \in \zeta} \mathrm{Adv}_{\mathcal{A}}.$$

For example, ζ can consist of all non-adaptive adversaries or adaptive adversaries. Note that in the rest of the paper, when we mention the advantage of an adversary, we mean his best advantage. We now recall Decorrelation Theory by first giving the definition of the *d-wise distribution matrix*.

Definition 2. *[Vau03] Let F be a random function from $\mathcal{M}_1$ to $\mathcal{M}_2$. The d-*wise distribution matrix *$[F]^d$ of F is a $|\mathcal{M}_1|^d \times |\mathcal{M}_2|^d$-matrix which is defined by $[F]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)} = \Pr_F[F(x_1) = y_1, \ldots, F(x_d) = y_d]$, where $x = (x_1, \ldots, x_d) \in \mathcal{M}_1^d$ and $y = (y_1, \ldots, y_d) \in \mathcal{M}_2^d$.*

There are two main notions of matrix-norms used in this theory and recalled in the following definition.

Definition 3. *[Vau03] Let $M \in \mathbb{R}^{|\mathcal{M}_1|^d \times |\mathcal{M}_2|^d}$ be a matrix. Then, two matrix-norms are defined by*

$$\|M\|_\infty = \max_{x_1,\ldots,x_d} \sum_{y_1,\ldots,y_d} |M_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}|,$$
$$\|M\|_A = \max_{x_1} \sum_{y_1} \cdots \max_{x_d} \sum_{y_d} |M_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}|.$$

Vaudenay [Vau03] defines the *decorrelation of order d for a random function F* as the distance between its d-wise distribution matrix and the d-wise distribution matrix of the ideal random function F^*, namely $\mathcal{D}([F]^d, [F^*]^d)$, where $\mathcal{D}$ denotes one of the measures of distance given above. Deciding which matrix-norm to use depends on the type of distinguisher envisaged. While $\|\cdot\|_\infty$ is used for non-adaptive distinguishers, $\|\cdot\|_A$ is used for adaptive distinguishers. When $\mathcal{D}([F]^d, [F^*]^d) = 0$, F is called a *perfect d-decorrelated function*. Now, the following lemma relates the best advantage of a distinguisher with the decorrelation distance.

Theorem 4 (Theorems 10 and 11 in [Vau03]). *Let F and F^* be a random function and the ideal random function, respectively. The respective advantages of the best d-limited non-adaptive and adaptive distinguishers, $\mathcal{A}_{\mathsf{NA}(d)}$ and $\mathcal{A}_{\mathsf{A}(d)}$, are*

$$\mathrm{Adv}_{\mathcal{A}_{\mathsf{NA}(d)}}(F, F^*) = \frac{1}{2}\|[F]^d - [F^*]^d\|_\infty$$

and,

$$\mathrm{Adv}_{\mathcal{A}_{\mathsf{A}(d)}}(F, F^*) = \frac{1}{2}\|[F]^d - [F^*]^d\|_A.$$

We recall one of the main theorems of this theory proving that if a cipher has decorrelation of order $2d$, then it is secure against a non-adaptive iterated attack of order d.

Theorem 5 (Theorem 18 in [Vau03]). *Let C be a random cipher on a message space $\mathcal{M}$ of size M such that $\|[C]^{2d} - [C^*]^{2d}\|_\infty \leq \varepsilon$, for some*

given $d \leq M/2$, where C^* is the ideal random cipher. Let us consider a non-adaptive iterated distinguisher of order d between C and C^* with n iterations. We assume that the distinguisher generates sets of d plaintexts of independent and identically distributed in all iterations. Then, we can bound the advantage of the adversary as

$$\mathrm{Adv}_{\mathcal{A}_{\mathsf{NAI}(d)}} \leq 5\sqrt[3]{\Big(2\delta + \frac{5d^2}{2M} + \frac{3\varepsilon}{2}\Big)n^2} + n\varepsilon,$$

where δ is the probability that any two different iterations send at least one query in common.

Lastly, we will remind the notion of *indicator function*.

Definition 6. *Let S be the sample space and $E \subseteq S$ be an event. The indicator function of the event E, denoted by $\mathbf{1}_E$, is a random variable defined as*

$$\mathbf{1}_E(s) = \begin{cases} 1, & \text{if } \ s \in E, \\ 0, & \text{if } \ s \notin E. \end{cases}$$

The indicator function can shortly be denoted as $\mathbf{1}_E$ instead of $\mathbf{1}_E(s)$. In the sequel, we define more general distinguishers, namely *adaptive* plaintext-ciphertext iterated distinguishers of order d.

3 Adaptive Plaintext-Ciphertext Iterated Distinguishers of Order d

In this section, we recall two generic distinguishers, namely an *adaptive* plaintext-ciphertext d-limited distinguisher (see Figure 2) and an *adaptive* plaintext-ciphertext iterated distinguisher of order d (see Figure 3). Both distinguishers are adaptive in a way that the adversary adaptively asks for both encryption and decryption of the queries. Herein we formalize these distinguishers.

We first define a *compact* function G to be distinguished. The goal of defining this function is to specify the input to the oracle to be either encrypted or decrypted (as the adversary makes either the plaintext queries or the ciphertext queries in a specific order depending on his type of attack).

Let $\mathcal{G}$ be the set of functions G such that $G : \mathcal{M} \times \{0,1\} \to \mathcal{M}$ satisfying $G(G(x,0),1) = x$ and $G(G(x,1),0) = x$, for all x. We denote $G_0(x) = G(x,0)$ and $G_1(x) = G(x,1)$ and point out $G_1^{-1} = G_0$ and $G_0^{-1} = G_1$. In what follows, G denotes a random element of $\mathcal{G}$ and G^* is a uniformly distributed element of $\mathcal{G}$.

Input: a function $\mathcal{F}$, a test $\mathcal{T}$, a distribution $\mathcal{R}$ on $\{0,1\}^*$
Oracle: the oracle Ω implementing either an instance of G or an instance of G^*

Pick $r \in \{0,1\}^*$ at random from $\mathcal{R}$
Set $u_1 = (a_1, b_1) \leftarrow \mathcal{F}(\cdot; r)$
Set $v_1 = \Omega(u_1)$
Set $u_2 = (a_2, b_2) \leftarrow \mathcal{F}(v_1; r)$
Set $v_2 = \Omega(u_2)$
...
Set $u_d = (a_d, b_d) \leftarrow \mathcal{F}(v_1, \ldots, v_{d-1}; r)$
Set $v_d = \Omega(u_d)$

Output $\mathcal{T}(v_1, \ldots, v_d; r)$

Fig. 2. A generic adaptive plaintext-ciphertext d-limited distinguisher

An adaptive d-limited distinguisher. The adversary $\mathcal{A}_{\mathsf{A}(d)}$ detailed in Figure 2 has access to an oracle Ω which implements either an instance of G or an instance of G^*, such that G_0 and G_1 perform encryption and decryption, respectively. He picks a random coin r from $\{0,1\}^*$ according to a given distribution $\mathcal{R}$ and queries a function $\mathcal{F}$ which is fed with r and the output of the previous queries $(v_1, v_2, \ldots, v_{i-1})$, where $v_k = \Omega(u_k)$ for all $k \in \{1, 2, \ldots, i-1\}$, and $1 \leq i \leq d$. He then receives a new query u_i. He sends this input u_i to the oracle to receive the output v_i, where –as explained– $v_i = \Omega(u_i)$. Finally, using a test $\mathcal{T}$, he outputs a decision bit "1" if he guesses that Ω implements an instance of the random function G or "0" if he guesses that Ω implements an instance of the ideal random function G^*.

Input: an integer n, a function $\mathcal{F}$, a test $\mathcal{T}$, a set $\mathcal{A}cc$, a distribution $\mathcal{R}$ on $\{0,1\}^*$
Oracle: the oracle Ω implementing a function G or G^*

for $k = 1$ **to** n
  Set T_k (with independent coins) $\leftarrow$ output of Distinguisher in Figure 2
end for
Output $1_{\mathcal{A}cc}(T_1, \ldots, T_n)$

Fig. 3. A generic adaptive plaintext-ciphertext iterated distinguisher of order d

An adaptive iterated distinguisher of order d. The iterated distinguisher given in Figure 3 is simply the iteration of the d-limited distinguisher (see Figure 2) in a way that the adversary $\mathcal{A}_{\mathsf{AI}(d)}$ repeats the distinguisher n

times, then he checks whether the output of n iterations are accepted or not with respect to a set $\mathcal{A}cc$. This gives his final decision.

Input: an integer n, a set X, differences Δ and ∇
Oracle: the oracle Ω implementing a permutation c

for $k = 1$ **to** n
  Pick x_1 uniformly at random from the set X
  Set $x_2 = x_1 \oplus \Delta$
  Set $y_1 = c(x_1)$, $y_2 = c(x_2)$
  Set $y_3 = y_1 \oplus \nabla$, $y_4 = y_2 \oplus \nabla$
  Set $x_3 = c^{-1}(y_3)$, $x_4 = c^{-1}(y_4)$
  Set $T_k = \mathbf{1}_{x_3 \oplus x_4 = \Delta}$
end for
if $T_1 + \cdots + T_n \neq 0$ **then**
  Output 1
else
  Output 0

Fig. 4. Boomerang Distinguisher

The Boomerang Attack [Wag99] defined in Figure 4 is an example for an adaptive plaintext-ciphertext iterated distinguisher of order d (see Figure 3) for the case $d = 4$. The adversary queries two (chosen) plaintexts and receives their corresponding ciphertexts, he then constructs two ciphertexts depending on the previous ciphertexts and asks for their decryption. The adaptively chosen queries to the oracle in each iteration of the Boomerang Attack [Wag99] can be written as $(u_1, u_2, u_3, u_4) = ((x_1, 0), (x_1 \oplus \Delta, 0), (c(x_1) \oplus \nabla, 1), (c(x_1 \oplus \Delta) \oplus \nabla, 1))$, where x_1 is selected uniformly at random over the set X, and Δ and ∇ denote non-zero differences.

4 Advantage of Adaptive Plaintext-Ciphertext Iterated Distinguishers of Order d

Vaudenay [Vau03] found a bound for the advantage of non-adaptive iterated distinguishers of order d, which is not apposite for the adaptive adversaries. We extend his result and provide a bound for the advantage of *adaptive* plaintext-ciphertext iterated distinguishers of order d. Strictly speaking, we compute the maximum success of the adversary who is making d adaptive queries to the oracle in each iteration to distinguish a random cipher $2d$-decorrelated upon using the $\|\cdot\|_A$ norm.

Theorem 7. *Let $G \in \mathcal{G}$ be a random function from $\mathcal{M} \times \{0,1\}$ to $\mathcal{M}$ such that $||[G]^{2d} - [G^*]^{2d}||_A \leq \varepsilon$, for some given $d \leq M/2$, where G^* is the ideal random cipher and $|\mathcal{M}| = M$. Let us consider* an adaptive *iterated distinguisher of order d $\mathcal{A}_{\mathsf{AI}(d)}$ who is trying to distinguish G from G^* by performing n iterations (see Figure 3). Then, the advantage* $\mathrm{Adv}_{\mathcal{A}_{\mathsf{AI}(d)}}$ *of $\mathcal{A}_{\mathsf{AI}(d)}$ is bounded as*

$$\mathrm{Adv}_{\mathcal{A}_{\mathsf{AI}(d)}} \leq 5\sqrt[3]{\Big(2\theta + e^{8d^2/M} + \frac{2d^2}{M} + \frac{3\varepsilon}{2} - 1\Big)n^2} + n\varepsilon,$$

where θ is the expected value of the probability that any two different iterations send at least one query in common for a given G.

Proof. Let one iteration consist of the input queries $u = (u_1, u_2, \ldots, u_d)$ and the output queries $v = (v_1, v_2, \ldots, v_d)$, where $u_i = (a_i, b_i)$ and $v_i = \Omega(u_i)$, for $1 \leq i \leq d$.

We first make two *observations* about the adaptive adversary.

Observation 1: *Inner-collisions* in input queries, i.e., $u_i \neq u_j$, are not allowed, since calling the same query twice in the same iteration will not give any advantage to the adversary.

Observation 2: Let $(u_i = (a_i, b_i), v_i)$ and $(u_j = (a_j, b_j), v_j)$ be two queries in the same iteration. *Cross inner-collisions* are not allowed, that is, we *never* have $a_i = v_j$ and $b_i \neq b_j$. Getting the same information will not give any advantage to the adversary.

Notice that these aforementioned observations do not hold between *different* iterations.

We begin similarly to the proof of Theorem 5 provided in [Vau03]. We first define $T(g)$ to be the probability that the test function $\mathcal{T}$ outputs 1 when $G = g$ (resp. $G^* = g$), i.e.,

$$T(g) = \mathbb{E}_r[\mathcal{T}(v_1, \ldots, v_d; r) | G = g].$$

We let p (resp. p^*) be the probability of the distinguisher outputting 1, let $\mathcal{A}cc$ be the acceptance set, and $T_k(G)$ (resp. $T_k(G^*)$) be the output of iteration k. Then we have

$$p = \mathsf{Pr}_G[(T_1(G), \ldots, T_n(G)) \in \mathcal{A}cc].$$

Notice that all $T_k(G)$'s are *pairwise independent* except that all are only dependent on G, and $T_k(G) = T(G)$. Hence, we obtain

$$p = \mathbb{E}_G\left[\sum_{(t_1,\ldots,t_n)\in\mathcal{A}cc} T(G)^{t_1+\cdots+t_n}(1 - T(G))^{n-(t_1+\cdots+t_n)}\right].$$

Then, p can be rewritten as

$$p = \sum_{k=0}^{n} a_k \mathbb{E}_G[T(G)^k (1 - T(G))^{n-k}],$$

for some integers a_k such that $0 \leq a_k \leq \binom{n}{k}$. Similarly, we have the same argument for p^*, i.e., $p^* = \sum_{k=0}^{n} a_k \mathbb{E}_{G^*}[T(G^*)^k (1 - T(G^*))^{n-k}]$.

The advantage of the distinguisher, $|p - p^*|$, is maximal when all a_k's are either 0 or $\binom{n}{k}$ depending on the distributions $T(G)$ and $T(G^*)$. Hence, we assume that $\mathcal{A}cc$ of the best distinguisher is of the form

$$\mathcal{A}cc = \left\{ (t_1, \ldots, t_n) \Big| \sum_{k=1}^{n} t_k \in \mathcal{B} \right\},$$

for some set $\mathcal{B} \subseteq \{0, \ldots, n\}$. Thus, we rewrite $p = \mathbb{E}_G[s(T(G))]$, where $s(x) = \sum_{k \in \mathcal{B}} \binom{n}{k} x^k (1 - x)^{n-k}$.

Now, consider the derivative of s which can be written as

$$s'(x) = \sum_{k \in \mathcal{B}} \binom{n}{k} \frac{k - nx}{x(1 - x)} x^k (1 - x)^{n-k}.$$

Notice that since the sum over all k, such that $0 \leq k \leq n$, is the derivative of $(x + (1 - x))^n$, then the total sum is zero. Hence, we obtain

$$|s'(x)| \leq \sum_{nx \leq k \leq n} \binom{n}{k} \frac{k - nx}{x(1 - x)} x^k (1-x)^{n-k} \leq \frac{n}{x} \sum_{nx \leq k \leq n} \binom{n}{k} x^k (1-x)^{n-k},$$

since $nx \leq k \leq n$. We note that when $x \geq 1/2$, we have $|s'(x)| \leq 2n$. Similarly, when $x < 1/2$, we have $|s'(x)| \leq 2n$. Hence, we get $|s'(x)| \leq 2n$, for every x. So, according to the Mean Value Theorem, we have

$$|s(T(G)) - s(T(G^*))| \leq 2n |T(G) - T(G^*)|.$$

Furthermore, Theorem 4 gives the exact advantage for the best *adaptive* d-limited distinguisher. Hence, $|\mathbb{E}_G[T(G)] - \mathbb{E}_{G^*}[T(G^*)]| \leq \varepsilon/2$ is obtained. We here notice that in Vaudenay's proof for Theorem 5, the non-adaptive case was considered which leads the same result.

We now define a new random variable $T^2(G)$ which is the output of another test with $2d$ entries, that is,

$$\mathcal{T}(v_1, \ldots, v_d; r) \times \mathcal{T}(v'_1, \ldots, v'_d; r').$$

Thanks to Theorem 4, we have $|\mathbb{E}_G[T^2(G)] - \mathbb{E}_{G^*}[T^2(G^*)]| \leq \varepsilon/2$. Hence, we get $|V(T(G)) - V(T(G^*))| \leq 3\varepsilon/2$ (obtained by combining $|\mathbb{E}_G[T(G)] - \mathbb{E}_{G^*}[T(G^*)]| \leq \varepsilon/2$ and $|\mathbb{E}_G[T^2(G)] - \mathbb{E}_{G^*}[T^2(G^*)]| \leq \varepsilon/2$). More precisely, we have

$$\begin{aligned}
&|V(T(G)) - V(T(G^*))| \\
&= |\mathbb{E}_G[T^2(G)] - \mathbb{E}_G^2[T(G)] - \mathbb{E}_{G^*}[T^2(G^*)] + \mathbb{E}_{G^*}^2[T(G^*)]| \\
&\leq |\mathbb{E}_G[T^2(G)] - \mathbb{E}_{G^*}[T^2(G^*)]| + |\mathbb{E}_G^2[T(G)] - \mathbb{E}_{G^*}^2[T(G^*)]| \\
&\leq \frac{3\varepsilon}{2}. \qquad (1)
\end{aligned}$$

In 1, we use $|\mathbb{E}_G[T(G)] + \mathbb{E}_{G^*}[T(G^*)]| \leq 2$, since $0 \leq T(G), T(G^*) \leq 1$.

Afterwards, the advantage of the distinguisher is

$$|p - p^*| = |\mathbb{E}_G[s(T(G))] - \mathbb{E}_{G^*}[s(T(G^*))]| \leq \mathbb{E}_{G,G^*}[|s(T(G)) - s(T(G^*))|].$$

By using Tchebichev's inequality, i.e., $\Pr[|T(G) - \mathbb{E}_G[T(G)]| > \lambda] \leq V(T(G))/\lambda^2$ and $\Pr[|T(G^*) - \mathbb{E}_{G^*}[T(G^*)]| > \lambda] \leq V(T(G^*))/\lambda^2$ for any $\lambda > 0$, we have

$$|p - p^*| \leq 5\sqrt[3]{\Big(2V(T(G^*)) + \frac{3\varepsilon}{2}\Big)n^2} + n\varepsilon, \qquad (2)$$

when $\lambda = \sqrt[3]{(2V(T(G^*)) + (3\varepsilon/2))/n}$.

So far, everything works similarly to [Vau03]. However, the rest is different since the function implemented in the oracle has new properties. For further details of the proof up to now, refer to [Vau03]. Now, it is left to bound $V(T(G^*))$.

Bounding $V(T(G^*))$. We now bound $V(T(G^*))$ by expanding it as

$$\begin{aligned}
&V(T(G^*)) = \\
&\sum_S \Pr_R[r] \Pr_R[r'] \Big(\Pr_{G^*}\left[(u,u') \xrightarrow{G^*} (v,v')\right] - \Pr_{G^*}[u \xrightarrow{G^*} v] \Pr_{G^*}[u' \xrightarrow{G^*} v'] \Big), \qquad (3)
\end{aligned}$$

where $S = \{(v,r),(v',r') \in \mathcal{T}\}$ and u (resp. u') is defined by both r and v (resp. r' and v'). For the sake of simplicity, we denote the expression $\Pr_R[r] \Pr_R[r'] \Big(\Pr_{G^*}\left[(u,u') \xrightarrow{G^*} (v,v')\right] - \Pr_{G^*}[u \xrightarrow{G^*} v] \Pr_{G^*}[u' \xrightarrow{G^*} v'] \Big)$ as P.

In order to find an upper bound for $V(T(G^*))$, we first divide Expression (3) into two *disjoint* sums depending on whether or not u and u' are

colliding, i.e., if there exist i and j such that $u_i = u'_j$. In detail, we have $S = S_1 \cup S_2$ such that $S_1 = \left\{(v,r),(v',r') \in \mathcal{T} |\ \exists i,j \text{ s.t. } u_i = u'_j\right\}$ and $S_2 = \left\{(v,r),(v',r') \in \mathcal{T} |\ \forall i,j \text{ s.t. } u_i \neq u'_j\right\}$. Thus, we write

$$\sum_{S} P = \sum_{S_1} P \ + \sum_{S_2} P.$$

We now bound each sum separately.

The sum over S_1, $\sum_{S_1} P$, is bounded as

$$\begin{aligned}
\sum_{S_1} P &\leq \sum_{v,v'} \sum_{r,r'} \Pr_R[r] \Pr_R[r'] \Pr_{G^*}\left[(u,u') \xrightarrow{G^*} (v,v')\right] \mathbf{1}_{S_1} \\
&= \sum_{g} \Pr[G^* = g] \sum_{v,v'} \sum_{r,r'} \Pr_R[r] \Pr_R[r'] \ \mathbf{1}_{(u,u') \xrightarrow{g} (v,v')} \ \mathbf{1}_{S_1} \\
&= \mathbb{E}_{G^*}[\Pr_{r,r'}[\exists i,j \text{ s.t. } u_i = u'_j |\ G]] \\
&\stackrel{def}{=} \theta,
\end{aligned}$$

where we denote $\mathbb{E}_{G^*}[\Pr_{r,r'}[\exists i,j \text{ s.t. } u_i = u'_j |\ G]]$ by θ. This can be interpreted as the expected value of the probability that any two iterations have at least one query in common for given G.

Now, we provide a bound for the sum over S_2, $\sum_{S_2} P$, which is for non-colliding inputs u and u'. We first note that since both G_0^* and G_1^* are from $\mathcal{M}$ to $\mathcal{M}$, and, hence, bijective, they are indeed the ideal cipher C^*, i.e., $G_0^* = G_1^* = C^*$. Therefore, their distribution matrices will be the same as the distribution matrix of the ideal cipher C^*. We define $x = (x_1, x_2, \ldots, x_d)$ and $y = (y_1, y_2, \ldots, y_d)$ as

$$x_i = \begin{cases} a_i, & \text{if } \ b_i = 0, \\ v_i, & \text{if } \ b_i = 1, \end{cases} \quad \text{and} \quad y_i = \begin{cases} v_i, & \text{if } \ b_i = 0, \\ a_i, & \text{if } \ b_i = 1, \end{cases}$$

where $u = ((a_1,b_1),(a_2,b_2),\ldots,(a_d,b_d))$, with $b_i \in \{0,1\}$, is the input tuple and $v = (v_1, v_2, \ldots, v_d)$ is its corresponding output tuple. This is basically collecting the plaintexts and ciphertexts into two separate tuples. Now, the sum over S_2 can be rewritten into three *disjoint* sums as

$$\sum_{S_2} A = \sum_{S_3} A + \sum_{S_4} A + \sum_{S_5} A.$$

Here, S_3, S_4 and S_5 are the three partitions of S_2, i.e., $S_2 = S_3 \cup S_4 \cup S_5$,
$S_3 = \Big\{(v,r),(v',r') \in \mathcal{T} \,|\, \forall i,j,k,m,e,f \ u_i \neq u'_j, x_k \neq x'_m, y_e \neq y'_f \Big\}$,
$S_4 = \Big\{(v,r),(v',r') \in \mathcal{T} \,|\, (\forall i,j,k,m \ u_i \neq u'_j, x_k \neq x'_m) \wedge (\exists e,f \ y_e = y'_f) \Big\}$,
$S_5 = \Big\{(v,r),(v',r') \in \mathcal{T} | (\forall i,j \ u_i \neq u'_j) \wedge (\exists k,m \ x_k = x'_m) \Big\}$, and A is
$\Pr_R[r] \Pr_R[r'] \Big(\Pr_{G_0^*}\left[(x,x') \xrightarrow{G_0^*} (y,y')\right] - \Pr_{G_0^*}[x \xrightarrow{G_0^*} y] \Pr_{G_0^*}[x' \xrightarrow{G_0^*} y'] \Big)$.
We now deal with these three sums.

The sum over S_3 (all non-colliding u's and u''s, all non-colliding x's and x''s, and all non-colliding y's and y''s), $\sum_{S_3} A$, can be rewritten as

$$\sum_{S_3} A \leq \frac{1}{2} \sum_{v,v'} \sum_{r,r'} A \times \mathbf{1}_{S_3} =$$
$$\frac{1}{2} \Big| \Pr_{G_0^*}\left[(x,x') \xrightarrow{G_0^*} (y,y')\right] - \Pr_{G_0^*}[x \xrightarrow{G_0^*} y] \Pr_{G_0^*}[x' \xrightarrow{G_0^*} y'] \Big| \sum_{v,v'} \sum_{r,r'} \Pr_R[r] \Pr_R[r'] \ \mathbf{1}_{S_3}. \tag{4}$$

Here, since $\Big| \Pr_{G_0^*}\left[(x,x') \xrightarrow{G_0^*} (y,y')\right] - \Pr_{G_0^*}[x \xrightarrow{G_0^*} y] \Pr_{G_0^*}[x' \xrightarrow{G_0^*} y'] \Big|$ is constant when there is no collision between x and x' and between y and y', in Equality (4), we take it out from the sum. Afterwards, since we never have $a_i = v_j$ and $b_i \neq b_j$ according to Observation 2, there will not be any inner-collisions in x.

Now, we bound Equality (4) as

$$\frac{1}{2} \Big| \Pr_{G_0^*}\left[(x,x') \xrightarrow{G_0^*} (y,y')\right] - \Pr_{G_0^*}[x \xrightarrow{G_0^*} y] \Pr_{G_0^*}[x' \xrightarrow{G_0^*} y'] \Big| \sum_{v,v'} \sum_{r,r'} \Pr_R[r] \Pr_R[r'] \ \mathbf{1}_{S_3}$$
$$\leq \frac{1}{2} \left(\frac{1}{M(M-1)\cdots(M-2d+1)} - \frac{1}{M^2(M-1)^2\cdots(M-d+1)^2} \right) M^{2d} \tag{5}$$
$$\leq \frac{e^{8d^2/M}}{2} - \frac{d(d-1)}{2M} - \frac{1}{2}. \tag{6}$$

Note that Inequality (5) is due to fact that the sum in (4) is bounded by the total number of v and v' which is M^{2d} and $P_1 \geq P_2^2$. The way to obtain Inequality (6) is shown in Appendix A.

On the other hand, the sum over S_4, $\sum_{S_4} A$, will be the sum over all colliding y's and y''s, all non-colliding x's and x''s, and all non-colliding u's and u''s. When x and x' are non-colliding, it is not possible to have

colliding y and y'. Hence, we have $\Pr_{G_0^*}\left[(x,x') \xrightarrow{G_0^*} (y,y')\right] = 0$. Therefore, the sum over S_4 will be negative, i.e., $\sum_{S_4} A \leq 0$.

Finally, we provide a bound for the sum S_5, $\sum_{S_5} A$, as

$$\begin{aligned}
\sum_{S_5} A &\leq \sum_{v,v'} \sum_{r,r'} \Pr_R[r] \Pr_R[r'] \Pr_{G^*}\left[(u,u') \xrightarrow{G^*} (v,v')\right] \mathbf{1}_{S_5} \\
&= \sum_{g} \Pr[G^* = g] \sum_{r,r'} \Pr_R[r] \Pr_R[r'] \mathbf{1}_{S_5} \qquad (7) \\
&= \mathbb{E}_{G^*}[\Pr_{r,r'}[\exists i,j \text{ s.t. } x_i = x'_j \mid \forall k,m \text{ s.t. } u_k \neq u'_m \text{ and } G]] \\
&\stackrel{def}{=} \gamma \\
&\leq \frac{d^2}{M}.
\end{aligned}$$

Here, we define $\gamma = \mathbb{E}_{G^*}[\Pr_{r,r'}[\exists i,j \text{ s.t. } x_i = x'_j \mid \forall k,m \text{ s.t. } u_k \neq u'_m \text{ and } G]]$ as the expected value of the probability that x and x' collide when G is given and there is no collision between u and u'. We get $\gamma \leq d^2/M$ which is proved in Appendix B. Notice that Equality (7) gives the probability γ explicitly.

Now, if we sum up all the results, then we have

$$V(T(G^*)) \leq \theta + \frac{e^{8d^2/M}}{2} + \frac{d^2}{M} - \frac{1}{2}$$

by setting $d/2M \leq d^2/2M$.

When we substitute $V(T(G^*))$ in (2), then we have

$$|p - p^*| \leq 5\sqrt[3]{\left(2\theta + e^{8d^2/M} + \frac{2d^2}{M} + \frac{3\varepsilon}{2} - 1\right)n^2} + n\varepsilon.$$

□

Allowing $\theta \approx \delta$ to compare Theorem 5 with Theorem 7, we observe that the bound for adaptive attacks is *higher* than the bound for non-adaptive attacks. This fact comes with no surprise. Adaptive adversaries are stronger than non-adaptive adversaries, in general, and adaptive queries can provide the adversary with some advantage.

5 Conclusion and Final Remarks

In this work, we study the resistance against adaptive plaintext-ciphertext iterated distinguishers of order d which has not been explored before. We

prove the bound for this distinguisher in which the adversary is making adaptive plaintext and ciphertext queries to the oracle depending on the previous queries. This work contributes to proving the security of previous and future designs based on Decorrelation Theory since previously there was no clue with adaptive iterated adversaries in this context.

It is worth mentioning that Theorem 7, provided in this paper, poses two questions. The theorem proves that decorrelation of order $2d$ is sufficient for a cipher to resist an iterated attack of order d. The first question asks whether or not this condition is necessary. The second question is as follows: can the probability θ of having the same query in different iterations increase the advantage of our adaptive adversary? Not surprisingly, similar questions were posed by Theorem 5. Bay et al. [BMV12] have recently answered these questions by providing two counterexamples that are not intuitive. Namely, Bay et al. proceeded as follows for the questions in Theorem 5.

- The first question is answered by showing that the decorrelation of order $2d$ is necessary. They provide a 3-round Feistel construction decorrelated to the order $2d-1$, that is $\|[C]^{2d-1} - [C^*]^{2d-1}\|_A \leq 2(2d-1)^2/q$, where q is the cardinality of the finite field $\mathsf{GF}(q)$. They then perform a successful non-adaptive iterated distinguisher of order d against this cipher.
- The second one is answered by providing again a 3-round Feistel construction decorrelated to the order $2d$ such that $\|[C]^{2d} - [C^*]^{2d}\|_A \leq 8d^2/2^k$, where 2^k is the number of elements in $\mathsf{GF}(2^k)$. They construct even an iterated distinguisher of order 1 on this cipher, when δ is high.

These counter-intuitive examples can also be applied to our case since the Feistel ciphers used in the solution to both questions are decorrelated by the adaptive norm, and non-adaptive attacks are a subset of adaptive attacks. To conclude, thanks to [BMV12], our two questions for Theorem 7 are immediately answered.

References

[BF06a] Thomas Baignères and Matthieu Finiasz. Dial C for Cipher. In Eli Biham and Amr M. Youssef, editors, *Selected Areas in Cryptography*, volume 4356 of *Lecture Notes in Computer Science*, pages 76–95. Springer, 2006.

[BF06b] Thomas Baignères and Matthieu Finiasz. KFC - The Krazy Feistel Cipher. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 380–395. Springer, 2006.

[BMV12] Asli Bay, Atefeh Mashatan, and Serge Vaudenay. Resistance against Iterated Attacks by Decorrelation Revisited. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO*, volume 7417 of *Lecture Notes in Computer Science*, pages 741–757. Springer, 2012.

[BV05] Thomas Baignères and Serge Vaudenay. Proving the Security of AES Substitution-Permutation Network. In Bart Preneel and Stafford E. Tavares, editors, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 65–81. Springer, 2005.

[CV94] Florent Chabaud and Serge Vaudenay. Links Between Differential and Linear Cryptoanalysis. In Alfredo De Santis, editor, *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 356–365. Springer, 1994.

[CW79] Larry Carter and Mark N. Wegman. Universal Classes of Hash Functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[CW81] Larry Carter and Mark N. Wegman. New Hash Functions and Their Use in Authentication and Set Equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.

[LR85] Michael Luby and Charles Rackoff. How to Construct Pseudo-Random Permutations from Pseudo-Random Functions (Abstract). In Hugh C. Williams, editor, *CRYPTO*, volume 218 of *Lecture Notes in Computer Science*, page 447. Springer, 1985.

[LR86] Michael Luby and Charles Rackoff. Pseudo-random Permutation Generators and Cryptographic Composition. In Juris Hartmanis, editor, *STOC*, pages 356–363. ACM, 1986.

[Nyb91] Kaisa Nyberg. Perfect Nonlinear S-Boxes. In Donald W. Davies, editor, *EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 378–386. Springer, 1991.

[PV98] Guillaume Poupard and Serge Vaudenay. Decorrelated Fast Cipher: An AES Candidate Well Suited for Low Cost Smart Card applications. In Jean-Jacques Quisquater and Bruce Schneier, editors, *CARDIS*, volume 1820 of *Lecture Notes in Computer Science*, pages 254–264. Springer, 1998.

[Vau98a] Serge Vaudenay. Feistel Ciphers with L_2-Decorrelation. In Stafford E. Tavares and Henk Meijer, editors, *Selected Areas in Cryptography*, volume 1556 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 1998.

[Vau98b] Serge Vaudenay. Provable Security for Block Ciphers by Decorrelation. In Michel Morvan, Christoph Meinel, and Daniel Krob, editors, *STACS*, volume 1373 of *Lecture Notes in Computer Science*, pages 249–275. Springer, 1998.

[Vau99a] Serge Vaudenay. Adaptive-attack Norm for Decorrelation and Super-Pseudorandomness. In Howard M. Heys and Carlisle M. Adams, editors, *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*, pages 49–61. Springer, 1999.

[Vau99b] Serge Vaudenay. On Probable Security for Conventional Cryptography. In JooSeok Song, editor, *ICISC*, volume 1787 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 1999.

[Vau99c] Serge Vaudenay. Resistance Against General Iterated Attacks. In Jacques Stern, editor, *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 255–271. Springer, 1999.

[Vau03] Serge Vaudenay. Decorrelation: A Theory for Block Cipher Security. *J. Cryptology*, 16(4):249–286, 2003.

[Wag99] David Wagner. The Boomerang Attack. In Lars R. Knudsen, editor, *FSE*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.

A Some Details of Bounding Expression 6

Hence, we will give the detailed upper bounding of the following expression

$$\frac{1}{2}\left(\frac{1}{M}\frac{1}{M-1}\cdots\frac{1}{M-2d+1}-\frac{1}{M^2}\frac{1}{(M-1)^2}\cdots\frac{1}{(M-d+1)^2}\right)M^{2d},$$

or equivalently,

$$\frac{1}{2}\left(\frac{1}{1-\frac{1}{M}}\frac{1}{1-\frac{2}{M}}\cdots\frac{1}{1-\frac{2d-1}{M}}\right)-\frac{1}{2}\left(\frac{1}{(1-\frac{1}{M})^2}\frac{1}{(1-\frac{2}{M})^2}\cdots\frac{1}{(1-\frac{d-1}{M})^2}\right).$$

In order to find an upper bound for Expression 6, we need to maximize $(1-1/M)^{-1}(1-2/M)^{-1}\cdots(1-(2d-1/M))^{-1}$. Hence, we use two inequalities such that $(1-1/x)^{-1}\leq 1+2/x$ when $|x|\geq 2$, which holds for $x=M$ since $M\geq 2$ according to Theorem 7 and $\left(1+r/k\right)^k\leq e^r$, when $1+r/k\geq 0$, then, the upper bound is

$$\frac{1}{1-\frac{1}{M}}\frac{1}{1-\frac{2}{M}}\cdots\frac{1}{1-\frac{2d-1}{M}}\leq e^{8d^2/M}.$$

In addition,we get

$$\frac{1}{(1-\frac{1}{M})^2}\frac{1}{(1-\frac{2}{M})^2}\cdots\frac{1}{(1-\frac{d-1}{M})^2}\geq 1+\frac{d(d-1)}{M}.$$

by using *geometric series formula*, i.e., $(1-x)^{-1}=\sum_{n=0}^{\infty}x^n$ for $|x|<1$, which implies that $(1-1/x)^{-1}\geq 1+1/x$ for $|x|>1$. Hence, we get the desired upper bound for Expression (6).

B Bounding the probability γ

We find an upper bound for γ which is the expected value of the probability that x and x' collide when G is given and there is no collision between u and u'. There is only one way for x and x' to collide when there is no collision between u and u'. This happens when one common query is from u (respectively u') and the other is from v' (respectively v). In detail, let $u_i=(a_i,b_i)$ and $u'_j=(a'_j,b'_j)$ be two respective entries from u and u', and v_i and v'_j be their corresponding output. When $b_i=0$, $b'_j=1$ and $a_i=v'_j$, then there is a collision in x and x' such that $x_i=x'_j$. Since u and v' are independent, the probability that u and v' collide is less than

$d^2/2M$. Similarly, we have the same result for u' and v. Thus, we bound γ as

$$\gamma \leq \frac{d^2}{2M} + \frac{d^2}{2M} = \frac{d^2}{M}.$$

C Linear and Differential Distinguishers

Input: an integer n, a set X, a distribution $\mathcal{X}$ on X, a set I, masks a and b
Oracle: an oracle Ω implementing a permutation c

for $i = 1$ **to** n
  Pick x_1 at random from $\mathcal{X}$
  Set $y_1 = c(x_1)$
  Set $T_i = a \cdot x_1 \oplus b \cdot y_1$
end for

if $T_1 + \cdots + T_n \in I$ **then**
  Output 1
else
  Output 0

Fig. 5. Linear Distinguisher

Input: an integer n, a set X, a distribution $\mathcal{X}$ on X, differences α and β
Oracle: an oracle Ω implementing a permutation c

for $i = 1$ **to** n
  Pick x_1 at random from $\mathcal{X}$
  Set $x_2 = x_1 \oplus \alpha$
  Set $y_1 = c(x_1)$, $y_2 = c(x_2)$
  Set $T_i = \mathbf{1}_{y_1 \oplus y_2 = \beta}$
end for

if $T_1 + \cdots + T_n \neq 0$ **then**
  Output 1
else
  Output 0

Fig. 6. Differential Distinguisher